We take it personally

Our vision, values and exceptional people contribute to our success

SAIC®

From Science to Solutions

Risk Assessment as a Key Component of an Information Security Architecture (ISA)

Lynda L. McGhie CISSP, CISM

Information Security Engineering Security Practice Manager
SAIC Commercial Business Services
State and Local Operation
Phone (530) 558-9574
e:mail: lynda.l.mcghie@saic.com

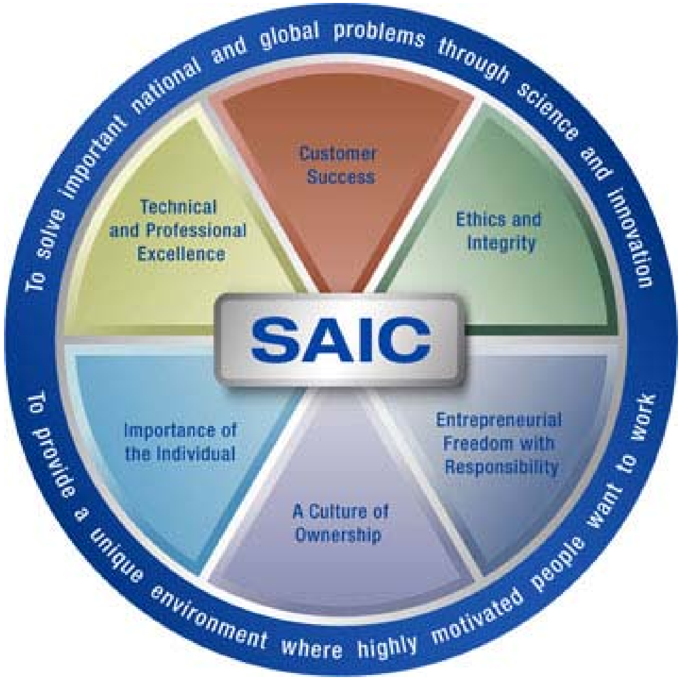
Agenda

- About SAIC
- Risk Management
- Risk Assessment
- Developing a Threat Profile
- Information Security Architecture

Our Company

For almost four decades, Science Applications International Corporation (SAIC) has created solutions for complex technical challenges worldwide. A Fortune 500® corporation, we are one of the leading systems, solutions and technical services companies worldwide.

Our Core Values & Purpose


To solve important national and global problems through science and innovation

Customer Success

Technical and Professional Excellence

Ethics and Integrity

SAIC

Importance of the Individual

A Culture of Ownership

Entrepreneurial Freedom with Responsibility

To provide a unique environment where highly motivated people want to work

Our Successes

37 years of continuous growth

- $8.3 billion in annual revenues for FY 2007
- Fortune 500® company – #298

Superb staff of qualified professionals

- More than 44,000 personnel worldwide
- 10,000 employees with advanced degrees
- 19,000 with security clearances

Key positions on initiatives of national importance

- National security
- Intelligence
- Homeland defense
- Cancer research

Leading provider of contracted R&D services

All figures current as of April 2007.

SAIC Security Engineering Practice

SAIC performs risk assessments and organizational effectiveness reviews to include:

- Identity and Access Management (authorization, authentication and administration Processes)
- Information security assessment and strategy
- Policy and procedure assessment and creation
- Training and awareness plans
- Communication plans
- Incident Monitoring and Response (IM&R) Strategy
- Computer Incident Response Teams (CIRT)/Process
- Security organization development, staffing and planning

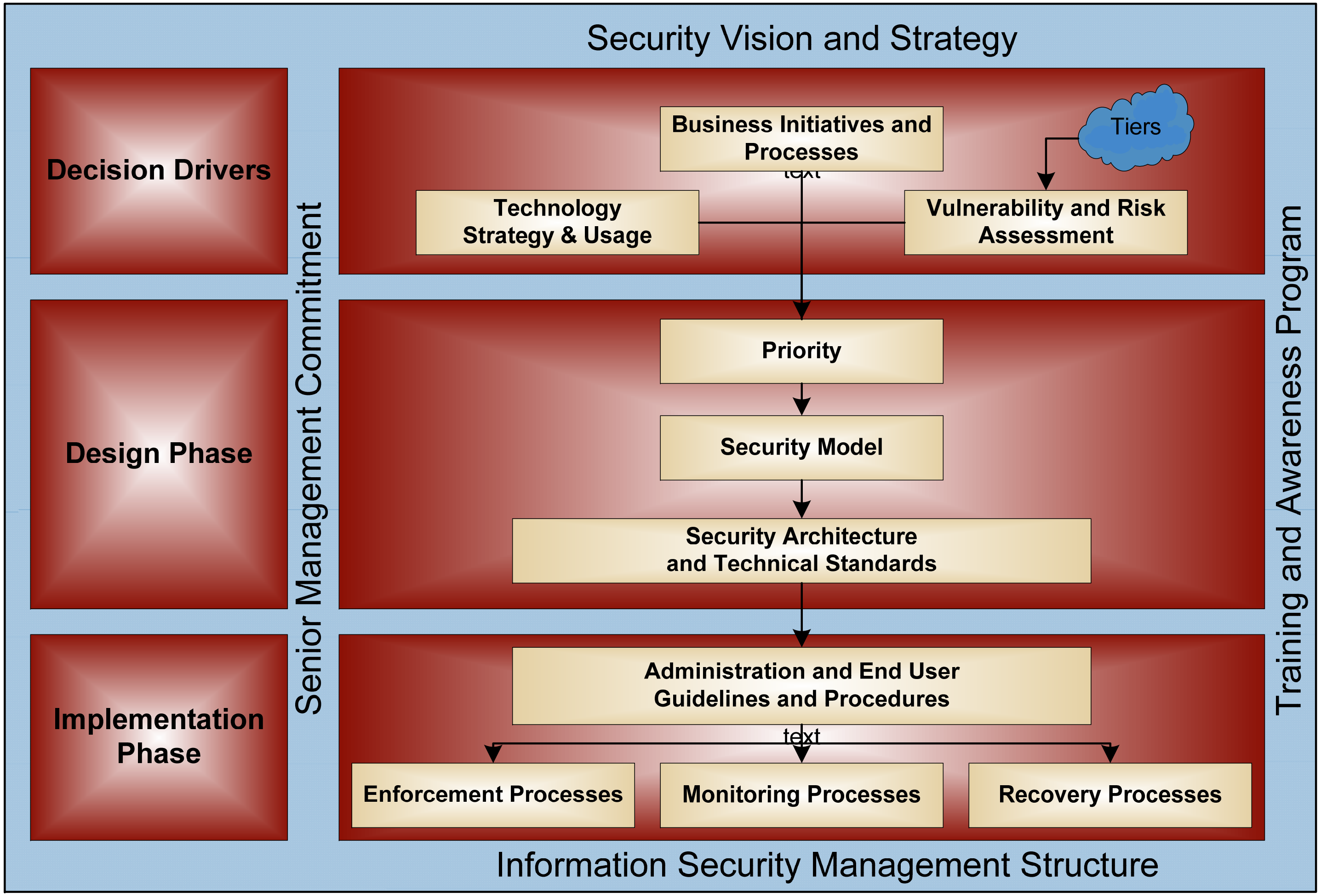
SAIC performs Information Security Management Services :

- Firewall and DMZ Architecture/Management
- Intrusion Detection and Prevention System (IDS/IPS)
- Secure remote access (wireless, laptops, PDAs)
- Virtual Private Network (VPN) Implementation
- Event aggregation, correlation and monitoring

SAIC Provides Ongoing Support Services for What we Design and Deliver

SAIC®
From Science to Solutions

How do the Key Components Work Together?



Security Vision and Strategy

Decision Drivers

Business Initiatives and Processes

Tiers

text

Technology Strategy & Usage

Vulnerability and Risk Assessment

Design Phase

Priority

Security Model

Security Architecture and Technical Standards

Implementation Phase

Administration and End User Guidelines and Procedures

text

Enforcement Processes

Monitoring Processes

Recovery Processes

Senior Management Commitment

Training and Awareness Program

Information Security Management Structure

From Science to Solutions

Risk Management – How Does it Apply to State Government?

- Risk management is a high priority for the State of California CISO and for SAM compliance.

- How does an ISO integrate a risk management policy and process into the department's or agency's overall information security and privacy program?

- How does an ISO integrate the RA process into an overall Information Security Architecture?

- This presentation will define and discuss the State of California's requirements for risk management and identify and discuss a path towards compliance with SAM and other CA state privacy requirements.

- The presentation will identify various risk assessment methodologies and approaches and recommend one that fits into the State of California requirements as well as industry best practices.

- This risk assessment model will then be superimposed on the Information Security Architecture model. The ISA components will also be discussed within the framework of risk management.

SAM – Risk Management

Risk Management Program Risk management is the process of identifying risk, assessing it, and taking steps to reduce it to an acceptable level. Although the overall purpose of risk management is to identify and avoid or minimize (mitigate) the impact of threats to information and technology assets, the main goal of the program should be to protect the agency and its ability to perform its mission, not just its IT assets.

Each agency must provide for the proper use and protection of its information assets. Accordingly, agencies should assign the management responsibilities of the risk management program to a unit or individual. SAM Section 5305.2 requires that each agency provide a minimum of the following practices:

- Organizational and Management
- Personnel
- Physical Security
- Information Integrity and Data Security
- Personal Computer Security
- Software Integrity

An effective risk management program should also mitigate risks associated with:

- Network security practices (SAM Section 5310)
- Threat management (SAM Section 5305.1)
- Disaster/operational recovery (SAM Section 5355.1)
- Appropriate use

SAM – Risk Management

In addition, the risk management program must be designed to:

- Protect all IT resources and information (both electronic and paper based) from unauthorized use, access, modification, loss, destruction, or disclosure;
- Ensure the physical security of the agency's resources;
- Provide and maintain a documented disaster/operational recovery plan;
- Ensure current policies and procedures are maintained regarding federal, state, and departmental mandates and guidelines;
- Identify, assess, and respond to the risks associated with information assets;
- Prevent misuse or loss of state agency information assets by establishing and maintaining a standard of due care; and,
- Preserve the ability to meet program objectives in the event of the unavailability, loss, or misuse of information assets by establishing and maintaining cost-effective risk management practices.

State Risk Assessment Requirements

- Information security is a critical issue for state agencies. Increased access to government information and services has been realized as the state increasingly moves its core activities to the Internet.

- State agencies play a unique role as the managers and caretakers of some of the largest collections of critical systems, applications, and databases. These systems, applications, and databases often house information which is subject to strict controls and protections by law, including the data collected, stored, shared, and transmitted that was once very difficult to obtain.

- SAM Section 5300-5399 requires that state agencies conduct periodic risk assessments, and submit a risk management certification, signed by its director.

- A simple checklist is provided as a tool or example, but not required, nor is it intended to cover all of the steps that an agency will need for its annual certification, but its use will provide a high-level view of an agency's security posture when measured against general information security practices.

What is a Risk Assessment?

- The purpose of the risk assessment is to assess the system's use of resources and controls (implemented and planned) to eliminate and/or manage vulnerabilities that are exploitable by threats to the organization. It will also identify any of the following vulnerabilities:

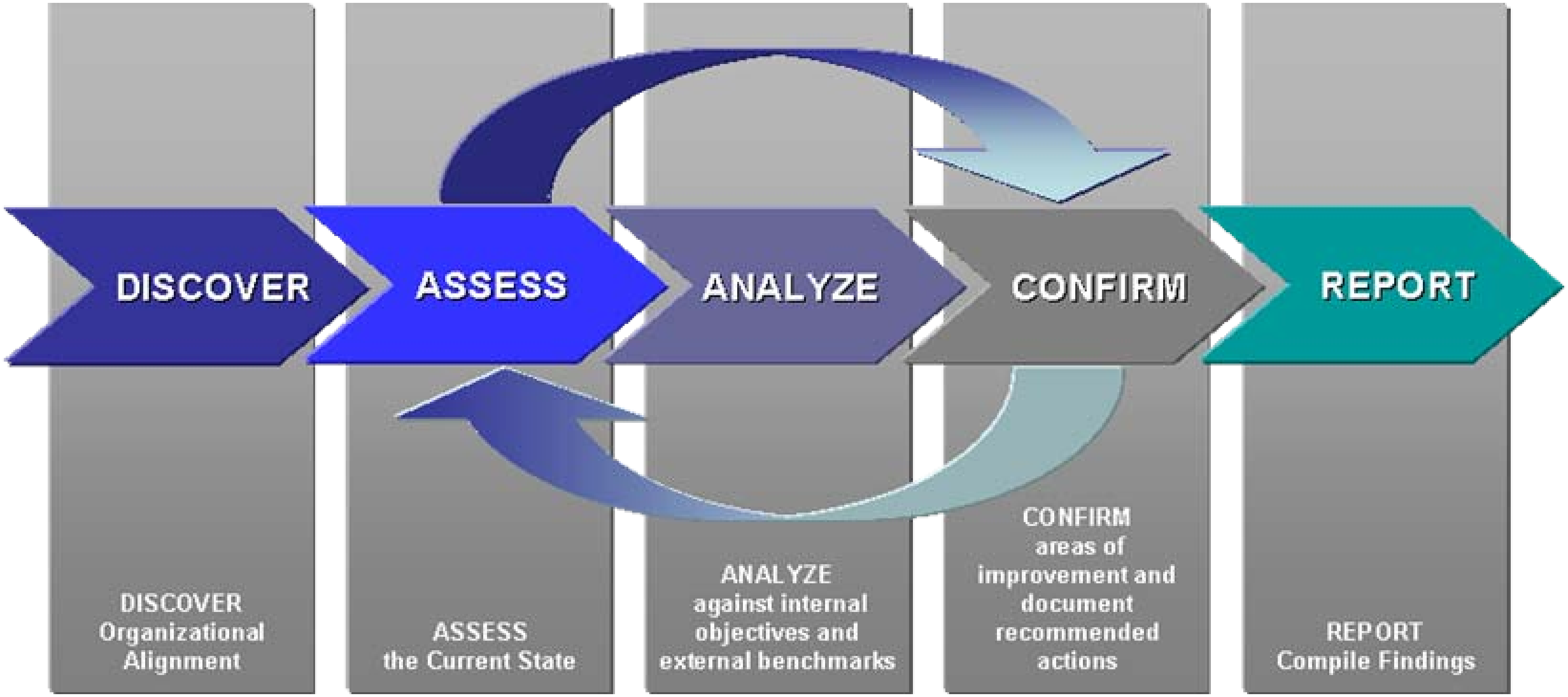
  - Risks associated with the system operational configuration
  - System's safeguards, threats and vulnerabilities
  - New threats and risks that might exist and, therefore, will need to be addressed after the current system is replaced
  - View the system relative to its conformance with corporate policies and procedures and all applicable legal and regulatory requirements

- The risk assessment should:

  - Provide a clear definition of the scope of the assessment such as present configuration, physical, environmental, personnel, telecommunications, and administrative security services provided
  - Identify which assets need to be protected and assign a value to each asset and label its business criticality.
  - Identify any and all threats.
    - Identified threats can be incorporated into a dynamic threat model/digital dashboard and integrated to other threat and vulnerability models, data, etc.

    Once identified, prioritize threats along with means to counter and respond to them

Risk Assessment Process



DISCOVER Organizational Alignment

ASSESS the Current State

ANALYZE against internal objectives and external benchmarks

CONFIRM areas of improvement and document recommended actions

REPORT Compile Findings

From Science to Solutions

Why Should You Do a Risk Assessment?

- A comprehensive integrated risk and vulnerability assessment will assist management in critical financial decisions as well as budgeting
- Since 911 everyone is increasingly concerned with safety of tenants and employees
- If you don't have an integrated risk assessment, how do you know what your security program should be, what to do first, second, etc.?
- How do you justify costs, resources, schedules, etc. without the output of a risk assessment?
- How do you know if you are compliant to legal and regulatory requirements?
- How do you know what an acceptable level of risk is for your department/agency and how do you communicate that and implement policies and procedures around that?
- Through the process of the risk, threat and vulnerability assessment you will learn and discover things about your environment that were previously unknown.
- Depending on time and available resources, quantitative and qualitative assessments both have value. There are pros and cons to each.

When Should You do a Risk Assessment?

- Your Department/Agency needs to certify a bi-annual enterprise risk assessment
- You have had an audit finding that needs resolution
- You have had a breach / other identified vulnerability
- You need to demonstrate compliance to legal and regulatory requirements
- You are making major enterprise architecture, infrastructure, or application changes
- You are initializing an Information Security and Privacy Program and need a baseline to establish a framework
- Other?

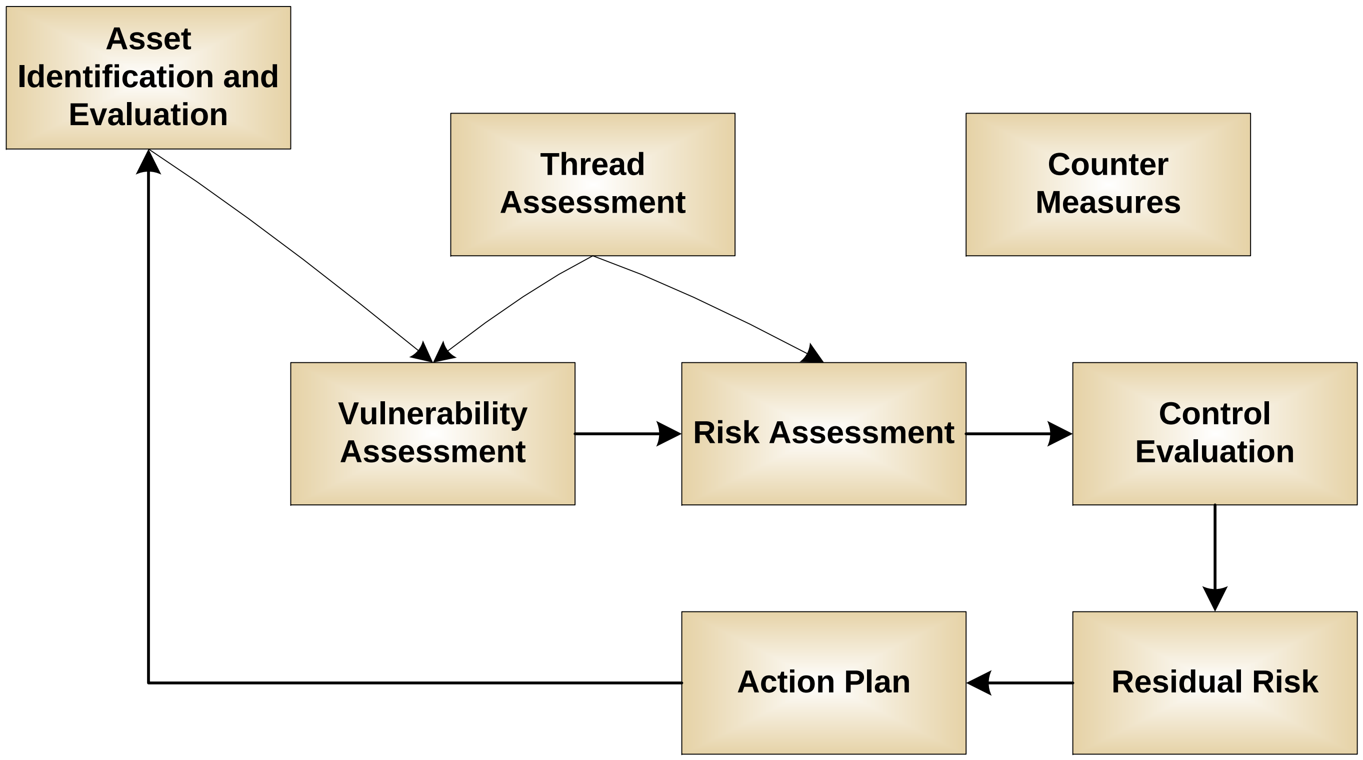
Determining Your Unique/Individual Risk Appetite

- To define your organization’s risk appetite and determine the acceptable level of risk, you should answer the following questions:
  - Where do we feel we should allocate our limited time and resources to minimize risk exposures? Why?
  - What level of risk exposure requires immediate action? Why?
  - What level of risk requires a formal response strategy to mitigate the potentially material impact? Why?
  - What events have occurred in the past, and at what level were they managed? Why?
- Each question is followed by a “why” because the organization should be able to articulate the quantitative and/or qualitative basis for the appetite, or it will come off as backwards-looking (based only on historical events) or even arbitrary.
- Develop a risk appetite table: Refer to – http://www.delcreo.com/delcreo/free/docs/RiskAppetiteTable.pdf

The RA Checklist

- The tool should be used in conjunction with the following steps:
  - This checklist should be completed by the agency's ISO, in cooperation with the CIO. A response to the items in each section should be prepared to accurately reflect the "point in time" picture of the agency's security posture.
  - Identify the levels of risk associated with any of the items that result in a no response.
  - Develop an appropriate action plan to mitigate, accept or transfer the identified risk.
  - For each identified risk where there is a remediation or mitigation plan, provide and get ISO approval for a corrective action plan and schedule and define a risk reassessment timeframe.
  - Define and implement a Risk Accountability Model.
  - Assign roles and responsibilities for implementing and monitoring timely completion of the action plan.
- This simple checklist is just one of several tools available to conduct information security risk assessments. More advanced risk assessment tools can be found on the State Information Security Office's Web site at www.infosecurity.ca.gov/risk/.

IT Risk Analysis Framework



Developing a Threat Profile

- Intentional, unintentional and natural threats

- Internal Vs. External Threats

- Threat – A threat is commonly described as an even with an undesired impact on the organization's assets.

    - Threat Agent – An event that may cause a threat to happen such as an earthquake or a disgruntled employee.
    - Undesirable Events – An undesirable event is what is caused by a threat agent.

- Begin by listing all threats by type such as Human, Nature and Technology.

- Developing a Threat Statement (Threat, Undesirable Event, Asset)

- Threat Model - A threat model is a description of the security aspects of a system under analysis. Usually the set of all possible attacks are identified and documented. Developing a threat model is commonly one of the first tasks associated with defining physical and logical controls for the organization.

    - Identify threats, Understand threats, categorize threats, identify mitigation strategies, test

Getting Started

- Develop a project plan and schedule (follow traditional project management discipline and methodology)
- Identify policies and guidelines to follow (SAM, FISMA, NIST, ISO 27002, COSO, CoBit, etc.
- Identify areas to be reviewed, measurement criteria and resources
- Decide on scoring methodology (quantitative or qualitative analysis)
- Identify other existing resources/inputs and how that information will factor in
  - Scorecards, metrics, audit findings, compliance assessments, incidents, vulnerability assessments, etc.
- Define output (reports, presentations, action plan, etc.)

Potential Pitfalls

- Scope Creep and changes in direction
- Delay in upfront data gathering process including both documents and interviews
- Getting the true picture and truthful information from interviewees
- Sponsor/stakeholders may not like some of the findings; what do you do?
- Other?

How does the Risk Assessment fit into the Overall Information Security Architecture?

What is an Information Security Architecture?

- An information security architecture (ISA) is the mechanism by which the confidentiality, integrity, and availability of an organization’s information assets are protected and by which protection responsibilities and requirements for these assets are communicated throughout the organization to include personnel, partners, third-parties, contractors, etc.

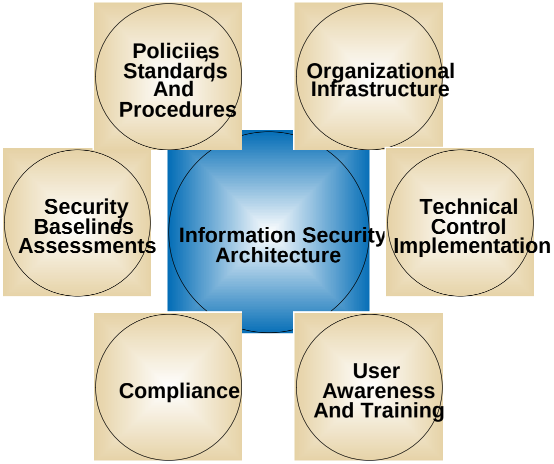
- The ISA is a concept that information security specialists have defined and designed to implement an enterprise wide security and privacy program. It is a management process intertwined into the day-to-day business operations of a company.

- The security and privacy life cycle consists of:

  - Performing security and risk assessments.
  - Developing an infrastructure to reduce the risk and meet defined security goals and objectives that support the business goals and objectives.
  - Implementing what has been developed.
  - Measuring the effectiveness of what has been implemented, and maintaining that infrastructure to meet the needs of the organization.

ISA Continued

- The ISA contains eight component parts:
  - Security Organization
  - Security Policies, Standards and Procedures
  - Technical Security Controls
  - Security Baselines/Risk Assessments
  - Security Awareness and Training Program
  - Compliance Management
  - Computer Incident/Emergency Response
  - Disaster Recovery/Business Continuity Planning/Performance Management


Policiies Standards And Procedures
Organizational Infrastructure
Security Baselines Assessments
Information Security Architecture
Technical Control Implementation
Compliance
User Awareness And Training

ISA Components

Security Organization - Defines the logical structure and functionality of the security organization. It details the roles and responsibilities of individuals and groups that are tasked with implementing information protection throughout the organization.

Security Policies, Standards, and Procedures - Details and summarizes the information security policies, procedures and standards.

Technical Security Controls – Discusses defense in-depth and layered security and privacy architectures.

Security Baselines/Risk Assessments - Discussion of the importance of a preliminary security assessment of a new system or a system that never has been assessed and the steps required to develop a baseline. This section also recommends a risk management program and testing methodology.

Security Awareness and Training Program - The importance and components of the Security Training and Awareness Program are discussed as well as the delivery mechanism. The security and privacy communication plan is also discussed in this section.

ISA Components

Compliance Monitoring - Compliance measures the extent which defined policies, standards, and procedures are followed by the organization. Compliance includes auditing, monitoring, and investigating at several levels of the organization. This section discusses the components and responsibilities of compliance assurance at the different levels of the organization and recommends a compliance, monitoring, and auditing program.

Computer Incident/Emergency Response - A description and explanation of best practices for the elements of a computer incident response practice. A recommended incident management program is recommended. An incident response methodology is provided and the basic response steps are defined. A forensic program is also outlined and integrated.

Disaster Recovery/Business Continuity Planning/Performance Management - This section details disaster recovery and business continuity planning within the organization. It makes recommendations for future improvements and also provides an outline of important performance considerations and measurements that should be implemented in a sound security and privacy program..

In Conclusion

- The ISA is necessary in today’s highly distributed “open” internet-based environments in which everyone inside and associated with the organization plays a role in security.

- Implemented controls are a combination of administrative, physical and technical procedures selected based on the types of threats and realistic risk related to an organization’s industry, market presence, and the technologies that have been implemented throughout the enterprise.

- The ISA begins at the strategic level through planning and support from executive management.

- The risk assessment process and subsequently risk management is a critical component of the overall ISA.

Cybersecurity No Longer a "Stepchild," says DHS Chief

As information technology boomed in the last two decades, the best young minds who grew up along with it flocked to developing the latest and greatest systems, not to protecting data and corporate networks. Cybersecurity was viewed as a “stepchild” of IT, U.S. artment of Homeland Security Secretary Michael Chertoff told cybersecurity professionals at a forum on cybersecurity. But today that dim view security is changing, “if it hasn’t changed already,” Chertoff said. As IT systems have become more sophisticated and the practice of cybersecurity has become more cutting edge, computer-savvy teens and twenty-somethings are now aspiring to master protection of electronic systems, Chertoff said. In his remarks, which preceded a panel of cybersecurity experts from such companies as Boeing, Bank of America, and General Electric, Chertoff made the case that companies should no longer consider IT threats a necessary cost of doing business. “We’ve entered an era of new threats and vulnerabilities,” he warned, and the consequences of failure are exponentially greater. Adversaries have matured along with the technology. State actors, criminals, and terrorists alike are increasingly motivated and capable, he said, and attacks are “increasing in frequency, sophistication, and scope.” Chertoff noted that the recent Russian military attacks in Georgia were coupled with Denial of Service (DoS) attacks launched against Georgian networks, which hindered Georgians’ ability to get information off the Web, thus throwing the population into confusion. Among Chertoff’s solutions on the government side is closing thousands of connection points between civilian government networks and the Internet, and he called for the public-private United States Computer Emergency Readiness Team (US-CERT) to validate security across the federal government’s civilian domains. *(Security Management 10/16/08)*